

Bonnie MacNaughton (Bar No. 107402)
Grant Damon-Feng (Bar No. 319451)
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, WA 98104
Telephone: (206) 622-3150
Facsimile: (206) 757-7700
Email: bonniemacnaughton@dwt.com
grantdamonfeng@dwt.com

John D. Freed (Bar No. 261518)
DAVIS WRIGHT TREMAINE LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111-6533
Telephone: (415) 276-6500
Facsimile: (415) 276-6599
Email: jakefreed@dwt.com

Attorneys for Plaintiffs
META PLATFORMS, INC., INSTAGRAM, LLC, and WHATSAPP LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

META PLATFORMS, INC., a Delaware
corporation, INSTAGRAM, LLC, a Delaware
limited liability company, and WHATSAPP
LLC, a Delaware limited liability company,

Plaintiffs,

v.

DOES 1-100,

Defendants.

Case No.

**COMPLAINT AND DEMAND FOR JURY
TRIAL**

COMPLAINT

Meta Platforms, Inc. (“Meta”) (formerly known as Facebook, Inc.), Instagram, LLC, and
WhatsApp LLC, allege the following against Defendants John Does 1-100:

I. INTRODUCTION

1. Since at least September 2019 and continuing to the present, Defendants have
engaged in a wide-ranging internet “phishing” scheme whereby they impersonate Facebook,
Messenger, Instagram, and WhatsApp in order to deceive users and steal their login credentials.
Defendants have created more than 39,000 websites purporting to be the login pages for

1 Facebook, Messenger, Instagram, or WhatsApp. On these websites, Defendants prompted users
2 to enter their usernames and passwords, which Defendants collected for their own benefit. As
3 part of their scheme, Defendants used services offered by Ngrok, Inc., to relay internet traffic to
4 their phishing websites in a manner that obfuscated where the websites were hosted. This has
5 enabled Defendants to conceal their identities and prolong their phishing attacks.

6 2. Plaintiffs bring this action to stop Defendants' unlawful and harmful conduct, and
7 to seek records to uncover the identities of the Doe Defendants. Defendants' conduct violates
8 Facebook's Terms of Service, California's Anti-Phishing Act, and the Lanham Act.

9 II. PARTIES

10 3. Plaintiff Meta is a Delaware corporation with its principal place of business in
11 Menlo Park, California. Meta, formerly known as Facebook, Inc., offers Facebook as a service
12 ("Facebook"). Meta also offers Messenger, an instant messaging app, as a service.

13 4. Plaintiff Instagram, LLC, a subsidiary of Meta, is a Delaware limited liability
14 company with its principal place of business in Menlo Park, California. The Instagram service
15 ("Instagram"), which is provided by Meta, and is a popular photo and video sharing social
16 networking service.

17 5. Plaintiff WhatsApp LLC, whose corporate parent is Meta, is a Delaware limited
18 liability company with its principal place of business in Menlo Park, California. The WhatsApp
19 service is a cross-platform mobile messaging app used across the globe. Meta acts as
20 WhatsApp's service provider for security-related issues.

21 6. Third-party Ngrok Incorporated ("Ngrok") is a cloud company that provides a
22 variety of services to software developers and technology professionals. Ngrok is a Delaware
23 corporation with its principal place of business in California and offers its services to customers
24 at a basic level for free or as a paid subscription for higher usage and functionality. Users of
25 Ngrok's free services can "publish" local websites to the publicly accessible internet using
26 unique web addresses (URLs) generated by Ngrok, while paid subscribers can create custom
27 URLs for their websites. These URLs all include the domain name ngrok.io.

V. FACTS

A. Background on Phishing Attacks

13. In this complaint, “phishing attacks” refers to the practice of deceiving internet users into divulging personal information using fraudulent websites and online impersonation. The Anti-Phishing Working Group (“APWG”), a nonprofit that works to stop phishing, reported that phishing attacks doubled in 2020 from the previous year. Anti-Phishing Working Group, Phishing Activity Trends Report, 2nd Quarter 2021 (Sept. 22, 2021), https://docs.apwg.org/reports/apwg_trends_report_q2_2021.pdf. In 2020, the FBI Internet Crime Complaint Center reported over 240,000 phishing scam complaints with losses totaling over \$54 million. Fed. Bureau of Investigation Internet Crime Complaint Center, Internet Crime Report 2020 (Mar. 17, 2021), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. In June 2021, the APWG recorded 222,127 phishing attacks in one month alone, the third-worst month in APWG’s reporting history. Social media companies were the second-most targeted industry in the second quarter of 2021, after financial institutions. *Id.*

B. Background on Plaintiffs.

14. Plaintiff Meta Platforms, Inc. is a Delaware corporation with its principal place of business in Menlo Park, California. Meta’s products include the Facebook, Messenger, Instagram, and WhatsApp apps.

15. Facebook is a social networking website and mobile application that enables its users to create their own personal profiles and connect with each other on their personal computers and mobile devices. Messenger is an instant messaging service provided by Meta that is available on mobile devices and desktop computers. Everyone who uses Facebook or Messenger must agree to Facebook’s Terms of Service (“ToS”). The Facebook ToS require everyone that uses Facebook or Messenger to agree not to use the services to do or share anything that: 1) “is unlawful, misleading, discriminatory, or fraudulent”; or 2) “infringes or violates someone else’s rights, including their intellectual property rights.” ToS § 3.2.1.

16. Instagram is a photo and video sharing and editing service, mobile application, and social network. Instagram users can choose to share their photos and videos with their

followers or with select groups of friends. They can also view, comment, and like posts shared on Instagram. Everyone who uses Instagram must agree to Instagram’s Terms of Use (“ToU”). The Instagram ToU prohibit using the service for doing “anything unlawful, misleading, or fraudulent or for an illegal or unauthorized purpose.” *Id.* Similarly, Instagram users cannot “sell, license, or purchase any account... or solicit, collect, or use login credentials ... of other users; or request or collect Instagram usernames [or] passwords.” *Id.*

17. WhatsApp is an encrypted messaging application that is used by people and businesses around the world to communicate and transact in a private way. In order to use WhatsApp, users must agree to the WhatsApp Terms and Policies (“WhatsApp Terms”). According to the WhatsApp Terms, users “must access and use our Services only for legal, authorized, and acceptable purposes.” *Id.* Users must not use or assist others in using WhatsApp in ways that are illegal, or “involve sending illegal or impermissible communications.” *Id.* Moreover, users must not (or assist others to) directly, indirectly, through automated or other means... exploit [WhatsApp] in impermissible or unauthorized manners, or in ways that ... harm us, our Services, systems, our users, or others.” *Id.* This prohibition applies to “gain[ing] or attempt[ing] to gain unauthorized access to our Services or systems [or] interfer[ing] with or disrupt[ing] the safety, security, confidentiality, integrity... of our Services.” *Id.*

C. Plaintiffs’ Intellectual Property


18. Meta¹, Instagram, and WhatsApp each developed trademarks they use to advertise and market products and services. Defendants used the following trademarks owned by Meta, Instagram, and WhatsApp in the phishing scheme (“the Trademarks”).

19. Plaintiffs duly registered the Trademarks with the United States Patent and Trademark Office on the Principal Register. True and correct copies of the registration certificates for the Trademarks are collectively attached hereto as Exhibit A.

MARK	REGISTRATION NO.	ISSUE DATE	INTERNATIONAL CLASS/ES
INSTAGRAM	4863595	12/01/2015	38

¹ Meta owns the trademarks for its Facebook and Messenger services. Instagram, LLC owns the trademarks for the Instagram service, and WhatsApp LLC owns the trademarks for the WhatsApp service.

1	INSTAGRAM	4856047	11/17/2015	42
2	INSTAGRAM	4827509	10/06/2015	45
3	INSTAGRAM	5566030	09/18/2018	42
4		4795634	08/18/2015	9, 38, 41, 42, 45
5				
6		4359872	07/02/2013	9, 38
7				
8				
9		5520067	07/17/2018	9, 38, 42, 45
10				
11	WHATSAPP	3939463	04/05/2011	42
12	WHATSAPP	4083272	01/10/2012	9, 38
13	WHATSAPP	5492738	06/12/2018	9, 38, 42, 45
14		3934743	03/22/2011	9, 35, 38, 41, 42, 45
15				
16	FACEBOOK	3814888	07/06/2010	42
17	FACEBOOK	3734637	01/05/2010	9, 38, 41, 42
18	FACEBOOK	3801147	06/08/2010	9, 38, 41, 42
19	FACEBOOK	3041791	01/10/2006	38
20	FACEBOOK	4471161	01/21/2014	41
21	FACEBOOK	4339123	05/21/2013	42
22	FACEBOOK	4392662	08/27/2013	45
23	FACEBOOK	4449195	12/10/2013	38
24	facebook	4099518	02/14/2012	38, 45
25	facebook	4102822	02/21/2012	38, 41, 42
26	facebook	4102823	02/21/2012	35, 42
27	facebook	4102824	02/21/2012	38, 45
28				

1 2 	4639783	11/18/2014	9, 38, 45
---	---------	------------	-----------

3 20. Plaintiffs' use of the Trademarks in interstate commerce has been extensive,
4 continuous, and substantially exclusive. Plaintiffs have made, and continue to make, a
5 substantial investment of time, effort, and expense in the promotion of their products and the
6 Trademarks. As a result of Plaintiffs' efforts and use, the Trademarks are inextricably linked
7 with the products and services offered by Plaintiffs.

8 **D. Defendants' Phishing Scheme**

9 21. Beginning no later than 2019, and continuing to the present, Defendants have
10 created and used over 39,000 websites to impersonate the login pages of Facebook, Messenger,
11 Instagram, and WhatsApp, and steal their users' login credentials (the "Phishing Websites").
12 Defendants used Ngrok to generate a URL for each of the Phishing Websites, and these bore one
13 or more of the Trademarks. On information and belief, Defendants disseminated these URLs to
14 their victims.² When victims visited the Ngrok URLs, they were directed to the Phishing
15 Websites, prompted to enter their requested credentials, and the credentials were collected by
16 Defendants.

17 22. On information and belief, Defendants published the Phishing Websites using
18 Ngrok's service because they did not need to register the URL with a domain registration
19 service, avoiding disclosure of identifying information and registration costs. Instead, Ngrok's
20 free service automatically generated URLs as a subdomain of Ngrok's domain ngrok.io (e.g.,
21 <https://d32831ea3827.ngrok.io/login.html>). This prevented Plaintiffs from identifying the real
22 locations of the Phishing Websites on the internet and being able to work with domain registrars
23 and hosting providers to take down the Phishing Websites at their source. The obfuscation of
24 Defendants' true hosting locations served to prolong and facilitate repeated phishing attacks.

25
26
27 ² See Cyble, *Ngrok Platform Abused by Hackers to Deliver a New Wave of Phishing Attacks*,
28 <https://blog.cyble.com/2021/02/15/ngrok-platform-abused-by-hackers-to-deliver-a-new-wave-of-phishing-attacks/>
(Feb. 15, 2021), Oussama Azrara, *Phishing on Facebook and Google with SET and Ngrok*,
<https://www.linkedin.com/pulse/phishing-facebook-google-set-ngrok-oussama-azrara/> (Feb. 9, 2020); Mocking
G33K, *Phishing with Ngrok*, <https://medium.com/@g33kxter/phishing-with-ngrok-252309890b87> (Mar. 10, 2018).

1 23. On information and belief, Defendants also published the Phishing Websites
2 using Ngrok because, for a fee, they could customize the URLs to deceive the victims. For
3 example, many URLs include Plaintiffs' Trademarks, which created the misleading impression
4 that the Phishing Websites originated from or are otherwise affiliated with Plaintiffs (*e.g.*,
5 <http://facebook.in.ngrok.io/>).

6 24. The following are examples of the Phishing Websites, followed by images of the
7 authentic Facebook, Messenger, Instagram, and WhatsApp websites that they impersonated:

8
9
10 ** Images on the following pages **
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Figure 1: Phishing Website using Ngrok URL <http://9747199d.ngrok.io/dashboard/>

The screenshot shows a phishing website designed to look like the Facebook login and sign-up page. At the top, the Facebook logo is on the left, and on the right, there are input fields for 'Email or Phone' and 'Password', with a 'Log In' button and a link for 'Forgotten account?'. Below the logo, the text 'Facebook helps you connect and share with the people in your life.' is followed by a graphic of a world map with orange person icons connected by lines. To the right of the map is the 'Create an account' section, which states 'It's quick and easy.' and includes input fields for 'First name', 'Surname', 'Mobile number or email address', and 'New password'. Below these are dropdown menus for 'Birthday' (set to 21 Sept 1994) and 'Gender' (with options Female, Male, and Custom). A 'Sign Up' button is prominently displayed. At the bottom, there is a language selection bar and a footer with various links like 'Sign Up', 'Log In', 'Messenger', etc., and the text 'Facebook © 2013'.

Figure 2: Authentic Facebook Login Page

The screenshot shows the authentic Facebook login and sign-up page. At the top, the Facebook logo is on the left, and on the right, there are input fields for 'Email' and 'Password', with a 'Log In' button, a checkbox for 'Keep me logged in', and a link for 'Forgot your password?'. Below the logo, the text 'Facebook helps you connect and share with the people in your life.' is followed by the same world map graphic with orange person icons. To the right is the 'Sign Up' section, which states 'It's free and always will be.' and includes input fields for 'First Name', 'Last Name', 'Your Email', 'Re-enter Email', and 'New Password'. Below these are dropdown menus for 'I am' (with a 'Select Sex' dropdown), 'Birthday' (with Month, Day, and Year dropdowns), and a link for 'Why do I need to provide my birthday?'. A 'Sign Up' button is prominently displayed. At the bottom, there is a language selection bar and a footer with various links like 'Mobile', 'Find Friends', 'Badges', etc., and the text 'Facebook © 2012 · English (US)'.

Figure 3: Phishing Website in Italian using Ngrok URL <http://facebook.in.ngrok.io/>

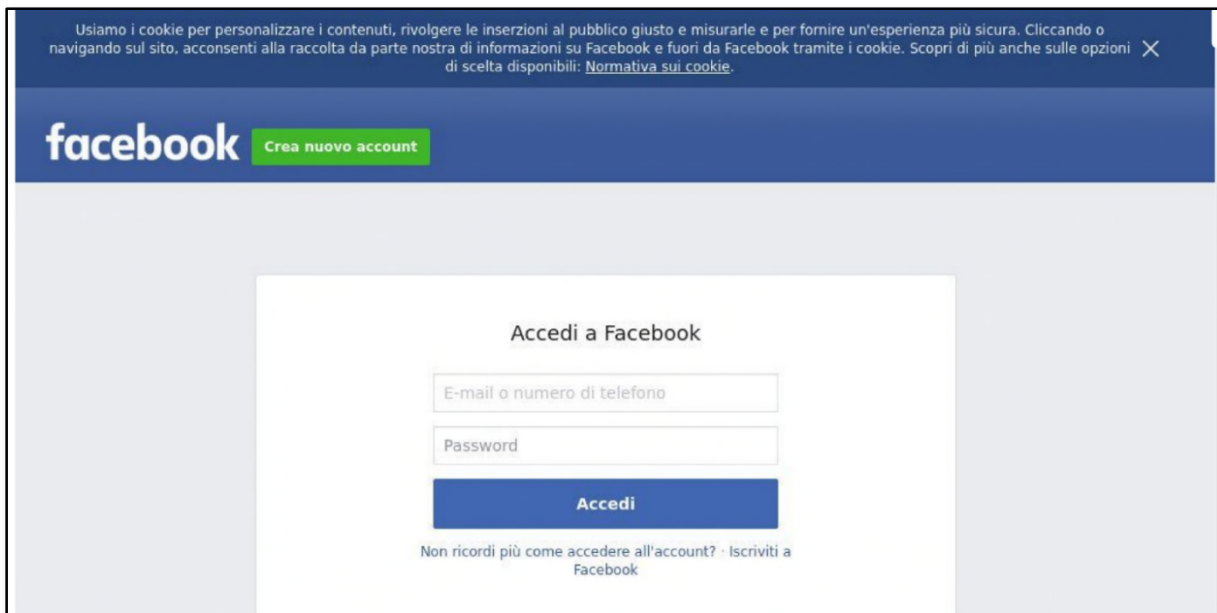


Figure 4: Authentic Facebook Login Page in Italian

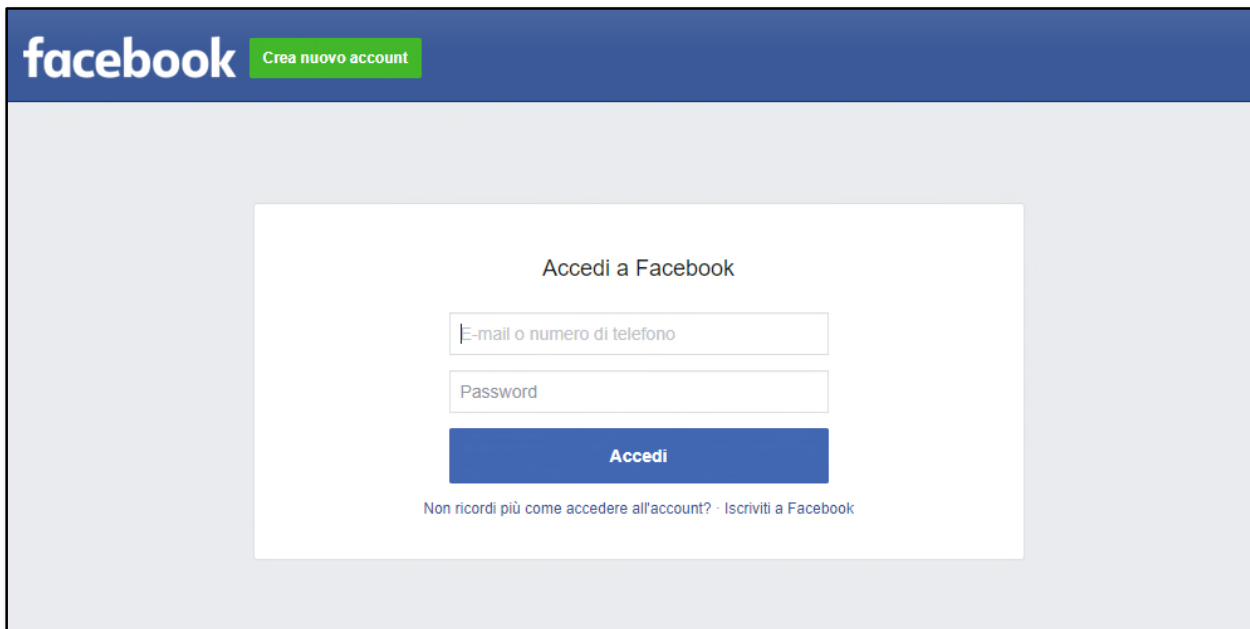
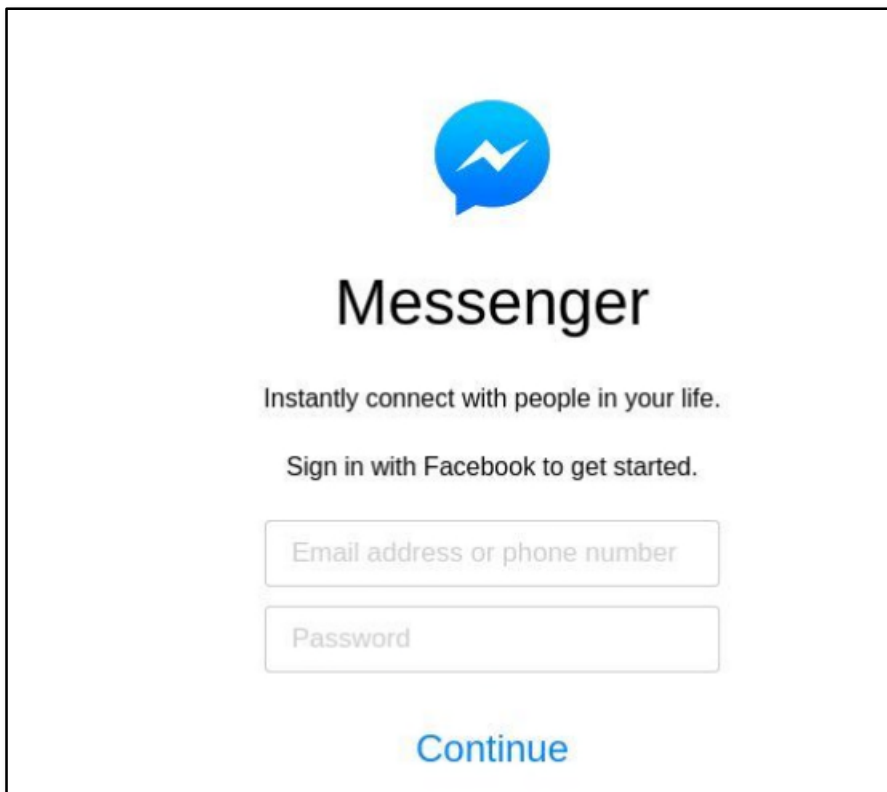
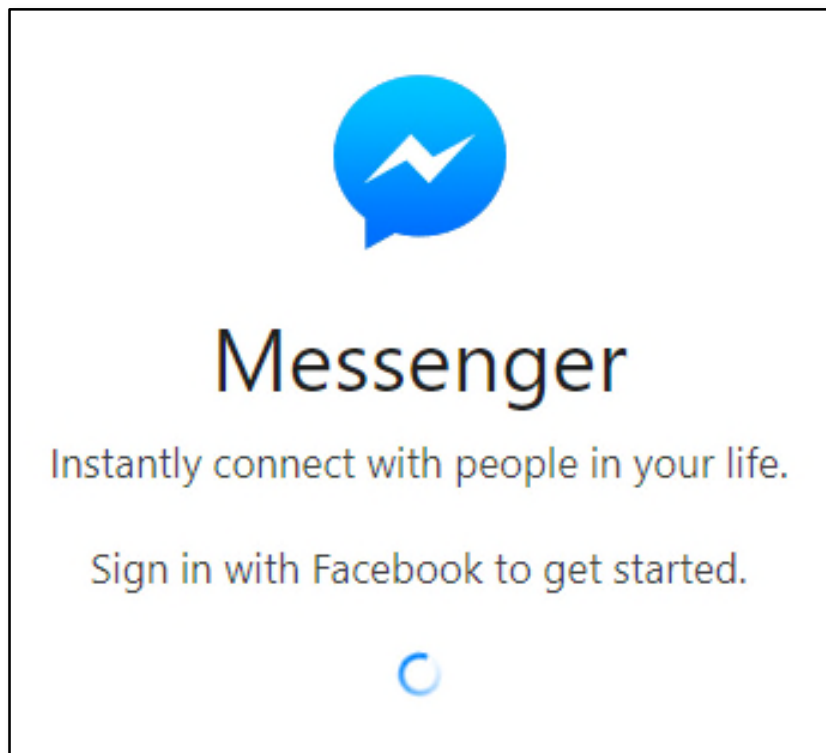


Figure 5: Phishing Website using Ngrok URL <https://d32831ea3827.ngrok.io/login.html>



The screenshot shows a phishing website designed to look like the Messenger login page. At the top is the Messenger logo, a blue speech bubble with a white lightning bolt. Below the logo is the word "Messenger" in a large, black, sans-serif font. Underneath that is the tagline "Instantly connect with people in your life." in a smaller, black, sans-serif font. Below the tagline is the text "Sign in with Facebook to get started." in a smaller, black, sans-serif font. There are two input fields: the first is labeled "Email address or phone number" and the second is labeled "Password". Both fields are empty and have a light gray border. Below the input fields is a blue button with the word "Continue" in white, sans-serif font.

Figure 6: Authentic Messenger Login Page



The screenshot shows the authentic Messenger login page. It features the same Messenger logo at the top. Below the logo is the word "Messenger" in a large, black, sans-serif font. Underneath that is the tagline "Instantly connect with people in your life." in a smaller, black, sans-serif font. Below the tagline is the text "Sign in with Facebook to get started." in a smaller, black, sans-serif font. At the bottom of the page is a blue circular loading spinner, indicating that the page is still loading or processing.

Figure 7: Phishing Website using Ngrok URL

<http://5989c7736ad8.ngrok.io/?php.sgnittes/moc.margatsni/>

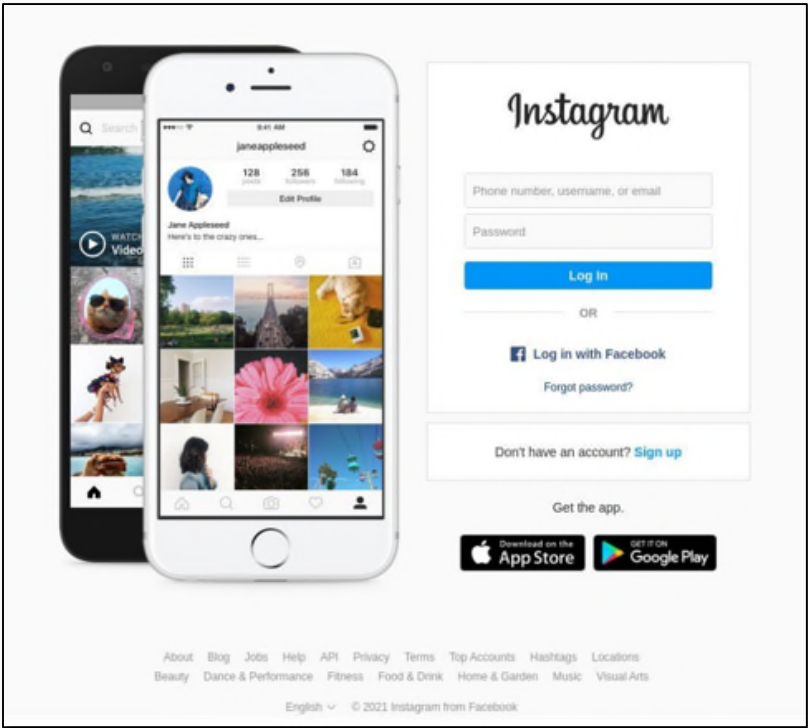


Figure 8: Authentic Instagram Login Page

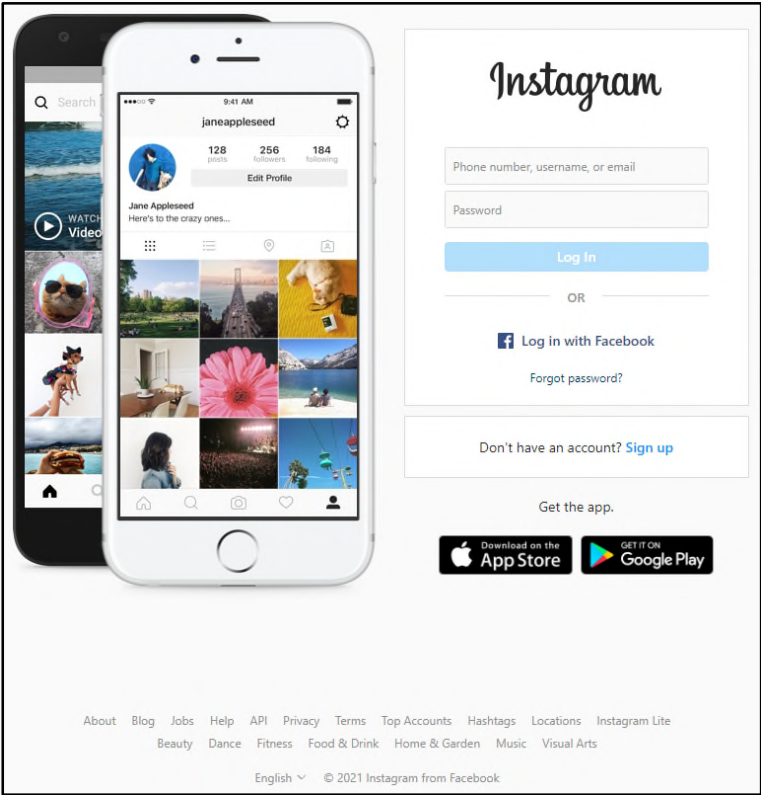


Figure 9: Phishing Website using Ngrok URL https://ce3568da7eeb.ngrok.io/login.html



Figure 10: Authentic Instagram Login Page



Figure 11: Phishing Website using Ngrok URL <https://38ad1bb93210.ngrok.io/>

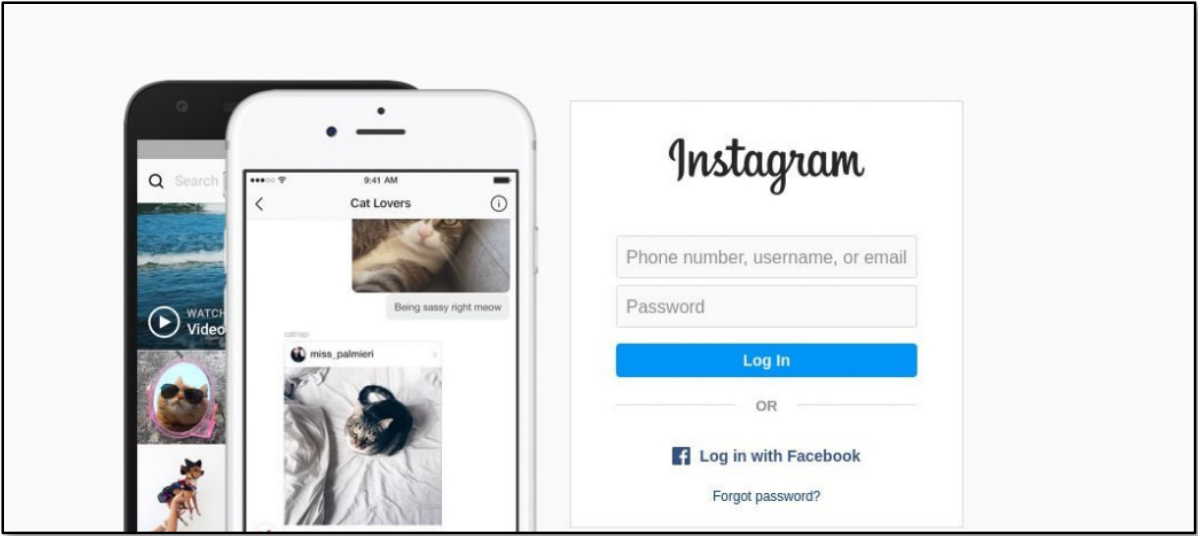


Figure 12: Authentic Instagram Login Page

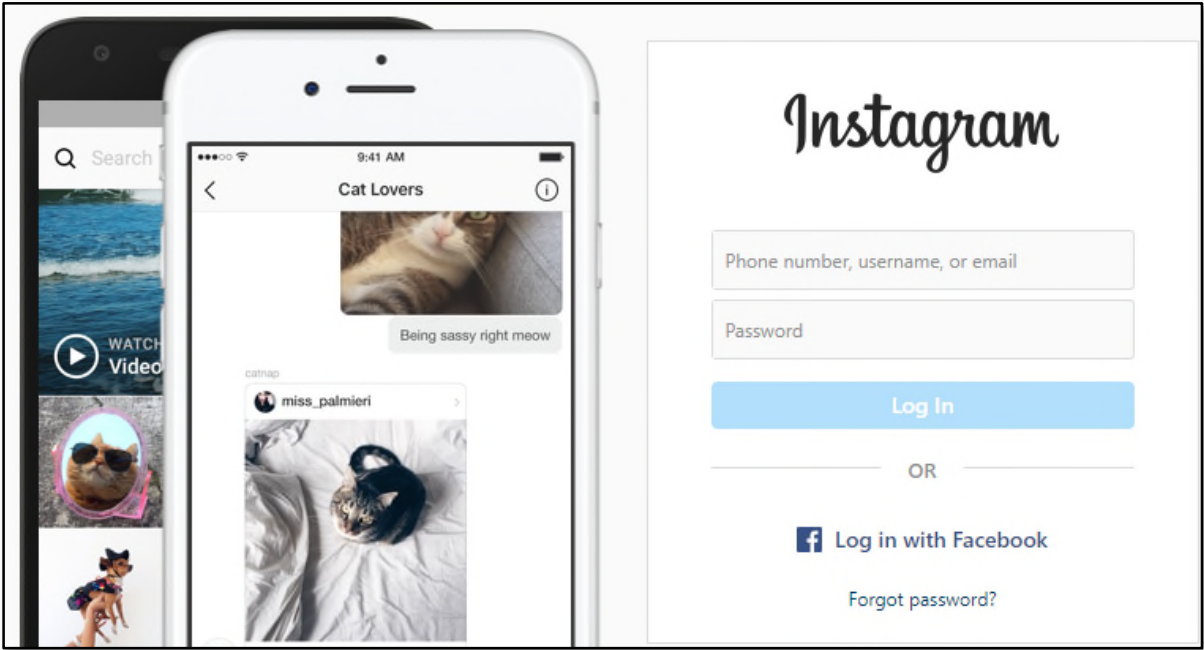


Figure 13: Phishing Website using Ngrok URL https://b71ef0393d7a.ngrok.io/

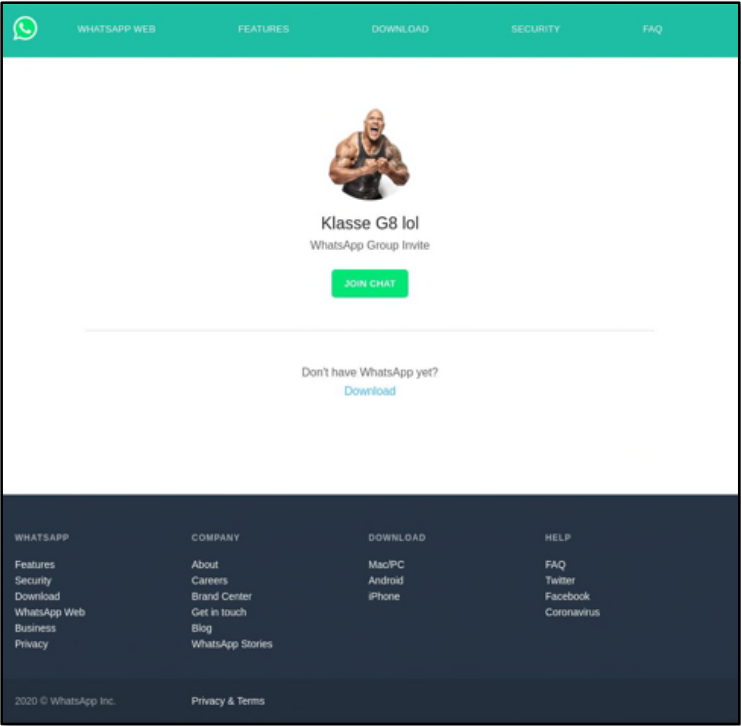
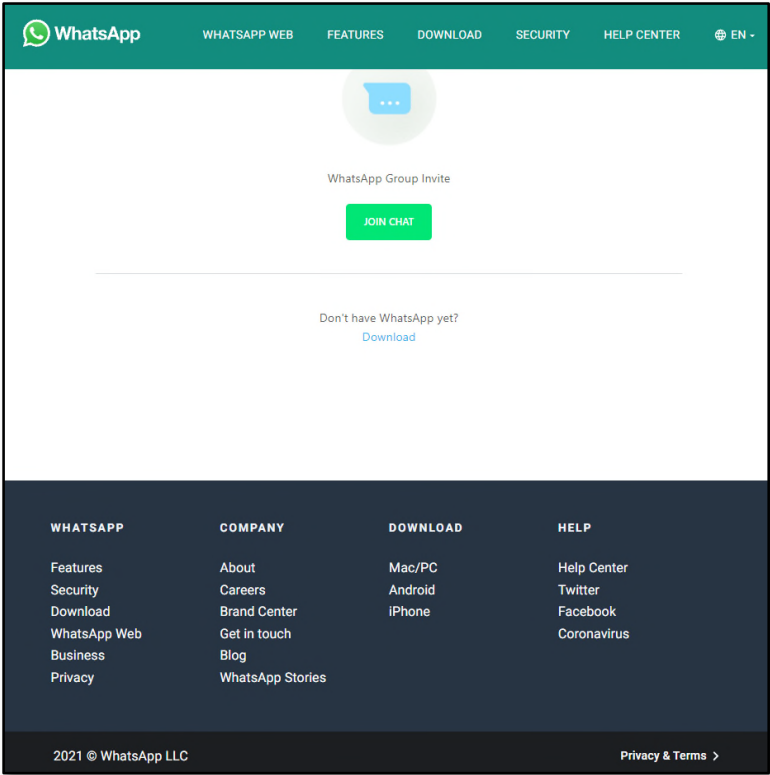


Figure 14: Authentic WhatsApp Login Page



VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

Anti-Phishing Act (Cal. Bus. & Prof. Code § 22948)

25. Plaintiffs re-allege and incorporate herein each paragraph above.

26. By creating and disseminating URLs for the Phishing Websites, Defendants falsely represented themselves to be Facebook, Messenger, Instagram, or WhatsApp, without Plaintiffs' authorization.

27. Defendants' Phishing Websites were intended to, and on information and belief did in fact, solicit, request, and induce users of Facebook, Messenger, Instagram, and WhatsApp to provide their account credentials.

28. Plaintiffs were adversely affected by Defendants' phishing scheme and suffered, without limitation, damage to their brands and reputations, harm to their users, and monetary losses in an amount to be determined.

29. Defendants' conduct constitutes a violation of Cal. Bus. & Prof. Code § 22948.3(a)(1).

30. As a result, Plaintiffs seek to recover the greater of their actual damages or five hundred thousand dollars (\$500,000) pursuant to Cal. Bus. & Prof. Code § 22948.3(a)(1). Further, because Defendants engaged in a pattern and practice of violating the Anti-Phishing Act, Plaintiffs request the trebling of their actual damages pursuant to Cal. Bus. & Prof. Code § 22948.3(c)(1). Plaintiffs further seek an award of their attorneys' fees and costs of suit pursuant to Cal. Bus. & Prof. Code § 22948.3(c)(2).

31. Plaintiffs further seek to enjoin Defendants' further violations of the Anti-Phishing Act for the reasons described in the following Causes of Action.

SECOND CAUSE OF ACTION

Breach of Contract (by Meta)

32. Plaintiff Meta re-alleges and incorporates herein each paragraph above.

43. As a result, Plaintiffs seek to recover Defendants' profits, treble actual damages, costs of the action, and attorneys' fees pursuant to 15 U.S.C. § 1117(a) and (b). Plaintiffs may also elect to seek statutory damages under 15 U.S.C. § 1117(c).

44. Plaintiffs are further entitled to injunctive relief pursuant to 15 U.S.C. § 1116. Plaintiffs have no adequate remedy at law for Defendants' wrongful conduct because, among other things: (a) the Trademarks are unique and valuable property that have no readily determinable market value; (b) Defendants' infringement of the Trademarks constitutes harm to Plaintiffs' reputation and goodwill such that Plaintiffs cannot be made whole by any monetary award; (c) if Defendants' wrongful conduct is allowed to continue, the public is likely to become further confused, mistaken, or deceived as to the source, origin or authenticity of the Phishing Websites; and (d) Defendants' wrongful conduct, and the resulting harm to Plaintiffs, is continuing.

FOURTH CAUSE OF ACTION

False Affiliation and Designation of Origin (15 U.S.C. § 1125(a))

45. Plaintiffs re-allege and incorporate herein each paragraph above.

46. The Trademarks are distinctive marks that are associated with Plaintiffs and exclusively identify their business, products, and services.

47. Defendants' continuous use in commerce of the Trademarks, and variations thereof, is likely to cause confusion, or to cause mistake, or to deceive the relevant public that the Phishing Websites are authorized, sponsored, or approved by, or are affiliated with, Plaintiffs.

48. Defendants' conduct constitutes false designation of origin in violation of 15 U.S.C. § 1125(a), entitling Plaintiffs to relief.

49. By reason of the above-described acts of Defendants, Plaintiffs have suffered damage to the goodwill associated with the Trademarks.

50. As a result, Plaintiffs seek to recover Defendants' profits, treble their actual damages, costs of the action, and attorneys' fees pursuant to 15 U.S.C. § 1117(a) and (b).

51. Plaintiffs further seek injunctive relief pursuant to 15 U.S.C. § 1116. Plaintiffs have no adequate remedy at law for Defendants' wrongful conduct because, among other things:

(a) the Trademarks are unique and valuable property that have no readily determinable market value; (b) Defendants' infringement of the Trademarks constitutes harm to Plaintiffs' reputation and goodwill such that Plaintiffs cannot be made whole by any monetary award; (c) if Defendants' wrongful conduct is allowed to continue, the public is likely to become further confused, mistaken, or deceived as to the source, origin or authenticity of the Phishing Websites; and (d) Defendants' wrongful conduct, and the resulting harm to Plaintiffs, is continuing.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray for the following relief:

A. That the Court enter judgment for Plaintiffs on all claims;

B. That the Court permanently restrain and enjoin Defendants, their directors, principals, officers, agents, representatives, employees, attorneys, successors and assigns, and all others in active concert or participation with them, from:

i. Accessing, or attempting to access, Plaintiffs' platforms and computer systems;

ii. Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Plaintiffs' platforms and computer system;

iii. Engaging in any activity that violates Meta's Terms, or facilitating others to do the same;

iv. Any infringing use of, or making or inducing others to infringe, any of Plaintiffs' trademarks including the Trademarks;

v. Sending any commercial electronic messages that contain any of Plaintiffs' trademarks, or otherwise representing that Defendants, either directly or by implication, are from or affiliated with Plaintiffs;

vi. Creating, operating, or maintaining any domains, subdomains, or URLs containing Plaintiffs' trademarks or which are confusingly similar to, or dilutive of, Plaintiffs' trademarks; and

vii. Assisting, aiding, or abetting any other person or business entity in

1 engaging in or performing any of the activities listed above.

2 C. That Plaintiffs be awarded damages, including but not limited to compensatory
3 damages, as permitted by law and in an amount to be proven at trial.

4 D. That Plaintiffs be awarded its costs, including reasonable attorneys' fees of this
5 action, and their reasonable attorneys' fees.

6 E. That the Court grant Plaintiffs such other, further, and additional relief as the
7 Court deems just and equitable.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all issues so triable pursuant to Rule 38(b) of the Federal Rules of Civil Procedure.

DATED this 20th day of December, 2021.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Plaintiffs

By s/ Bonnie E. MacNaughton
Bonnie E. MacNaughton, (Bar No. 107402)
Grant Damon-Feng (Bar No. 319451)
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, WA 98104
Telephone: (206) 622-3150
Facsimile: (206) 757-7700

John D. Freed (Bar No. 261518)
505 Montgomery Street, Suite 800
San Francisco, CA 94111-6533
Telephone: (415) 276-6500
Facsimile: (415) 276-6599

Platform Enforcement and Litigation
Jessica Romero
Stacy Chen
Jimmy Doan
Robert O'Loughlin